

#3
ST/JP2004/008942

日 本 国 特 許 庁
JAPAN PATENT OFFICE

26.07.2004

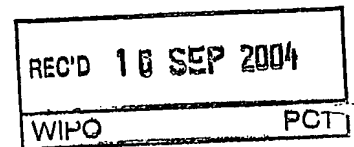
Rec'd PCT/PTO 04 APR 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年 6月19日

出 願 番 号
Application Number: 特願2003-175085
[ST. 10/C]: [JP2003-175085]



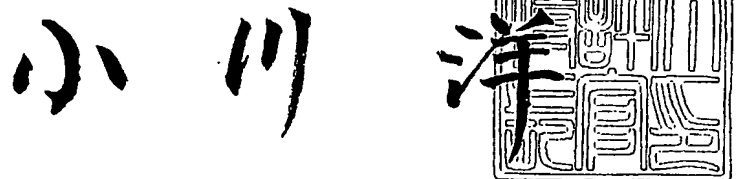
出 願 人
Applicant(s): 日本電信電話株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

2004年 9月 2日

特許庁長官
Commissioner,
Japan Patent Office



出証番号 出証特2004-3078667

【書類名】 特許願

【整理番号】 NTTH155516

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明者】

 【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

 【氏名】 小野 久美子

【発明者】

 【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

 【氏名】 立元 慎也

【発明者】

 【住所又は居所】 東京都千代田区大手町二丁目 3 番 1 号 日本電信電話株式会社内

 【氏名】 坂谷 精一

【特許出願人】

 【識別番号】 000004226

 【氏名又は名称】 日本電信電話株式会社

【代理人】

 【識別番号】 100077274

 【弁理士】

 【氏名又は名称】 磯村 雅俊

 【電話番号】 03-3348-5035

【選任した代理人】

 【識別番号】 100102587

 【弁理士】

 【氏名又は名称】 渡邊 昌幸

 【電話番号】 03-3348-5035

【手数料の表示】

【予納台帳番号】 013402

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701395

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体

【特許請求の範囲】

【請求項 1】 ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信により他の通信装置とのセッションを確立する通信装置において、

非対称鍵ペアを作成する手段と、

前記セッション制御サーバに対して前記非対称鍵ペアのうちの公開鍵に対する証明書発行を要求する要求手段と、

該セッション制御サーバから公開鍵証明書発行完了の通知を受信する受信手段と、

受信した公開鍵証明書を保管する保管手段と、

該セッション制御サーバに対して該通信装置の位置の登録要求を送信する送信手段と、

該セッション制御サーバから有効期間を含む位置登録完了の通知を受信する受信手段とを備え、

前記位置登録要求と証明書発行要求の一括した要求を送信することを特徴とする通信装置。

【請求項 2】 請求項 1 記載の通信装置において、

前記公開鍵証明書を保管する保管手段は、位置登録完了通知に含まれる有効期間を、発行された証明書の有効期間として保管することを特徴とする通信装置。

【請求項 3】 ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信により他の通信装置とのセッションを確立する通信装置において、

非対称鍵ペアを保管する手段と、

前記非対称鍵ペアのうちの公開鍵の証明書を保管する保管手段と、

前記セッション制御サーバに対して該公開鍵証明書の登録要求を送信する送信

手段と、

該セッション制御サーバに対して該通信装置の位置の登録要求を送信する送信手段と、

該セッション制御サーバから有効期間を含む位置登録完了の通知を受信する受信手段と

を備えたことを特徴とする通信装置。

【請求項 4】 請求項 3 記載の通信装置において、

前記公開鍵証明書を保管する保管手段は、位置登録完了通知に含まれる有効期間を、発行された証明書の有効期間として保管することを特徴とする通信装置。

【請求項 5】 ネットワークを介して複数の通信装置と通信可能に接続され、発信側の通信装置から送信された信号を受信し、受信された信号を着信側の通信装置に送信することで、前記発信側の通信装置と前記着信側の通信装置とのセッションを確立させるセッション制御サーバであって、

前記通信装置からの位置登録要求と、公開鍵に対する証明書発行要求あるいは証明書登録要求の一括した要求を受信する受信手段と、

前記要求を受け付け、公開鍵証明書の発行を行う、あるいは該公開鍵証明書の有効性を確認する手段と、

発行あるいは登録した該公開鍵証明書と位置情報を、有効期間とともに保管する手段と

を備えたことを特徴とするセッション制御サーバ。

【請求項 6】 請求項 5 記載のセッション制御サーバにおいて、

前記公開鍵証明書の問い合わせ要求を受信する受信手段と、

該公開鍵証明書の有効性を確認した上で、当該公開鍵証明書を通知する送信手段と

を備えたことを特徴とするセッション制御サーバ。

【請求項 7】 ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信システムにおいて、

非対称鍵ペアを作成する手段、公開鍵に対する証明書発行の要求を行う要求手段、証明書発行通知を受信する受信手段、公開鍵証明書を保管する保管手段、位

位置登録要求を送信する送信手段、および、有効期間を含む位置登録完了通知を受信する手段を備えた通信装置と、

前記通信装置からの位置登録要求を受信する受信手段、公開鍵に対する証明書発行あるいは証明書登録の要求を一括して受け付ける受信手段、証明書を発行あるいは有効性を確認する手段、および、発行あるいは登録した証明書と位置情報を、有効時間とともに保管する保管手段を備えたセッション制御サーバとを有することを特徴とする通信システム。

【請求項 8】 請求項 7 記載の通信システムにおいて、

前記通信装置は、位置登録完了通知に含まれる有効期間を発行された公開鍵証明書の有効期間として保管する保管手段を備え、

前記セッション制御サーバは、証明書問い合わせ要求を受信する受信手段と、証明書通知の送信手段を備えたことを特徴とする通信システム。

【請求項 9】 請求項 7 記載の通信システムにおいて、

前記通信装置は、非対称鍵ペアを保管する手段と、公開鍵証明書の登録要求を送信する送信手段を備え、

前記セッション制御サーバは、証明書問い合わせ要求を受信する受信手段と、証明書通知の送信手段を備えたことを特徴とする通信システム。

【請求項 10】 ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信方法において、

セッション制御サーバは、通信装置から位置登録と証明書発行の要求信号を受信すると、信号種別を判定し、位置登録要求であれば、証明書発行要求を含むか否かを判定し、発行要求を含む場合には、証明書を発行して、該位置情報と該証明書を管理するとともに、前記通信装置に対して位置情報と証明書発行完了通知の信号を送信することを特徴とする通信方法。

【請求項 11】 ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信方法において、

セッション制御サーバは、通信装置から証明書問合せ要求信号を受信すると、セッション制御を行うとともに、自ドメイン宛てか否かを判定し、そうであれば、信号種別を判定し、証明書問合せ要求であれば、証明書があるか否かを判定し

、あれば、該当する証明書を検索し、検索された証明書の有効性を確認して前記通信装置に対して証明書通知を送信し、自ドメイン宛てでない場合には、宛先のセッション制御サーバに該証明書問合せ要求信号を転送することを特徴とする通信方法。

【請求項 12】 ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信用プログラムであって、

セッション制御サーバのコンピュータに、通信装置から位置登録と証明書発行の要求信号を受信する手順、信号種別を判定する手順、位置登録要求であれば、証明書発行要求を含むか否かを判定する手順、発行要求を含む場合には、証明書を発行する手順、該位置情報と該証明書を管理する手順、前記通信装置に対して位置情報と証明書発行完了通知の信号を送信する手順を、それぞれ実行させるための通信用プログラム。

【請求項 13】 ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信用プログラムであって、

セッション制御サーバのコンピュータに、通信装置から証明書問合せ要求信号を受信する手順、セッション制御を行う手順、自ドメイン宛てか否かを判定する手順、そうであれば、信号種別を判定する手順、証明書問合せ要求であれば、証明書があるか否かを判定する手順、あれば、該当する証明書を検索する手順、検索された証明書の有効性を確認する手順、前記通信装置に対して証明書通知を送信する手順、自ドメイン宛てでない場合には、宛先のセッション制御サーバに該証明書問合せ要求信号を転送する手順を、それぞれ実行させるための通信用プログラム。

【請求項 14】 請求項 12 または 13 に記載の通信用プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子証明書発行およびその管理を行うセッション制御サーバと、その電子証明書を利用して通信を行う通信装置と、通信システムと、その通信方法

、ならびに、その通信方法を実行させるためのプログラムとそれを記録する記録媒体に関する。

【0002】

【従来の技術】

従来より、電子証明書の発行サーバ、電子証明書の管理サーバや認証局としては、LDAP (Lightweight Directory Access Protocol) サーバや、Web (World Wide Web) サーバが挙げられる。前者は、X.500ベースのディレクトリ管理データベースにアクセスするためのプロトコルであって、ディレクトリサーバ上のディレクトリ情報の作成、変更、削除、検索などの操作が可能である。後者は、インターネット上にハイパーテキストを構築し、あらゆる情報をアクセス可能にすることを目的としており、クライアントとサーバとの通信プロトコルにはHTTPが用いられる。

これらのサーバの利用方法では、電子証明書の利用者が、暗号化通信を行う場合に、必要に応じて通信相手の電子証明書を取得する必要がある。

また取得した電子証明書について、認証局リンクをたどったり、CRL (失効リスト) を取得するなどして、有効性を判断する必要もある。

【0003】

上記に関しては、インターネットの標準化機関であるIETF (Internet Engineering Task Force) がとりまとめている規格書の中で、RFC (Request for Comments) 2511 (非特許文献1参照) がある。

【0004】

【非特許文献1】

RFC 2511 Internet X.509 Certificate Request Message Format

【0005】

【発明が解決しようとする課題】

通信相手が複数の電子証明書を所持し、有効期間も様々である場合、電子証明

書の利用者は、セッションを開始する際に、どの電子証明書を利用するのが適当であるかを判断するために、電子証明書の管理サーバから、通信相手に対応する複数の電子証明書を取得して、各々について有効性を判断する必要があった。

また、有効であると判断した証明書を利用して、信号を送信しても、受信元の通信装置において、その証明書を利用可能な状態に設定していない場合には、受信側で復号化できず、セッション開始処理が遅延するという問題点があった。

さらに、通信相手のデジタル署名に含まれる電子証明書を受信した場合に、受信した証明書が有効か否かを判断するため、LDAPサーバに接続する処理などを行う場合には、セッションの開始処理が遅延するという問題点もあった。

【0006】

(目的)

本発明の目的は、上記のような従来の課題を解決し、セッション通信を行う通信装置に対して有効な電子証明書を配布でき、ユーザへのセッション確立時の有効性確認を容易にすることが可能な電子証明書管理機能を具備するセッション制御サーバ、およびそのサーバを用いて通信を行う通信装置と通信システムと通信方法、ならびにそのプログラムとそのプログラムを記録する記録媒体を提供することにある。

【0007】

【課題を解決するための手段】

本発明は、次のような機能を有する。

(1) あるユーザAが、自分の通信装置A'の位置登録要求を行うに当って、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求を一括してセッション制御サーバに送信する(請求項1参照)。

(2) セッション制御サーバが、通信装置A'から上記(1)の要求を受信し、ユーザ認証した上で証明書を発行し、位置情報の有効時間とともに保管する(請求項5参照)。

【0008】

(3) 上記(1)の処理を行った通信装置A'は、上記(2)の処理を行ったセッション制御サーバからの位置登録完了通知と、証明書発行完了通知を、有効時

間とともに受信し、これを保管する（請求項 2 参照）。

（4）あるユーザ A が、自分の通信装置 A' の位置登録要求を行うに当って、非対称鍵ペアとその鍵ペアの中の公開鍵に対する証明書を既に所有し、位置登録要求と、証明書登録要求を、一括してセッション制御サーバに送信する（請求項 3 参照）。

【0009】

（5）セッション制御サーバが、通信装置 A' から上記（2）の要求を受信し、証明書の有効性を判断して、ユーザ認証を行った上で、証明書の登録を有効時間のある位置登録とともに保管する（請求項 5 参照）。

（6）上記（4）の処理を行った通信装置 A' は、上記（5）の処理を行ったセッション制御サーバからの位置登録完了通知と、証明書発行完了通知を有効時間とともに受信し、これを保管する（請求項 4 参照）。

【0010】

（7）通信装置 B' がセッション開始に先立ち、通信相手 A の公開証明書をセッション制御サーバに対して問い合わせる。

（8）セッション制御サーバは、証明書問い合わせ要求を受信し、その問い合わせ対象の通信相手 A について、通信装置 A' の公開鍵証明書の有効性を確認し、これを通信装置 B' に通知する（請求項 6 参照）。

【0011】

本発明においては、位置情報の管理およびセッション制御を行うサーバが、電子証明書（公開鍵証明書）の管理を行うため、通信装置における実有効性を保証した配布が可能になる。

また、電子証明書の配布時には、位置情報の管理およびセッション制御を行うサーバにより有効性が確認されているため、セッション制御信号内で使用する電子証明書の有効性を、認証局などに問い合わせることなく、確認することが可能になる。

【0012】

【発明の実施の形態】

以下、本発明の実施の形態を、図面を参照して詳細に説明する。

(システム構成)

図1は、本発明の実施形態に係る通信システムの構成図である。

図1に示すように、通信システム100は、ネットワーク10を介して通信可能に接続された1台以上のセッション制御サーバ101と、複数の通信装置102を含むように構成されている。

また、通信装置102は、本発明による手順に従って、セッション制御サーバ101を介して暗号化通信により通信を行う。なお、通信システム100においては、セッション制御サーバ101が2台用意されているが、2台に限定されるものではない。また、通信装置102が2台用意されているが、2台に限定されるものではない。

【0013】

なお、本発明においては、通信装置102は、パソコン、携帯端末あるいはゲートウェイなどの通信機器を含み、ネットワーク10の構成は、有線、無線を問わない。

以降は、説明の便宜を図るために、通信装置102-1を発信側とし、通信装置102-2を着信側として説明する。セッション制御サーバ101-1を通信装置102-1を収容しているものとし、セッション制御サーバ101-2を通信装置102-2を収容しているものとして説明する。

セッション制御サーバ101-1、101-2がそれぞれ通信装置102-1と通信装置102-2から位置登録要求と公開鍵証明書の発行要求あるいは登録要求を受信し、位置登録情報と公開鍵証明書を保管する。

【0014】

(通信装置)

図2は、本発明の実施形態に係る通信装置のブロック構成図である。

図2に示すように、通信装置102は、信号送信手段110、セッション制御手段111、位置登録要求手段112、位置登録通知受信手段113、非対称鍵生成(保管)手段114、証明書発行(登録)要求手段115、位置情報と公開鍵証明書保管手段116、信号受信手段117および証明書通知受信手段118を含むように構成される。

ここで、114は、非対称鍵保管手段であるとともに、非対称鍵生成手段でもあり、また、115は証明書登録要求手段であるとともに、証明書発行要求手段でもある。従って、以後は、一方を括弧内にして並記する。なお、114、115は、これら一方だけの機能を備えたものであってもよい。

【0015】

通信装置102-1は、非対称鍵保管（生成）手段114で生成（保管）した公開鍵について、証明書登録（発行）要求手段115で要求信号を作成し、位置登録要求手段112で生成された位置登録要求信号とを合わせて、セッション制御手段111に送る。

セッション制御手段111で生成した信号を、信号送信手段110よりセッション制御サーバ101-1に送信する。

その後、セッション制御サーバ101-1から、位置登録完了通知信号を受信し、セッション制御手段111にて信号内容を解析し、位置登録通知受信手段113に送る。

公開鍵証明書が添付されていれば、証明書通知受信手段118で受信し、位置情報と公開鍵証明書保管手段116に、位置情報と公開鍵証明書を合わせて保管する。

これにより、通信装置102-1が使用可能な公開鍵証明書が入手できた状態となり、公開鍵を使用した暗号化情報を含む信号受信、および、公開鍵証明書を使用したデジタル署名を添付した信号送信が可能となる。

【0016】

（第1の実施形態）

第1の実施形態は、通信装置102-1がセッション制御サーバ101-1に対して位置登録+証明書発行を要求し、セッション制御サーバ101-1から位置登録と証明書発行の完了通知を受けるまでのやりとりである。

図4は、図2の通信装置における送信信号例を示す図、および、図5は、図2の通信装置における受信信号例を示す図である。

ここでの通信装置102-1の相手方は、勿論、セッション制御サーバ101-1である。例えば、図4に示す通信装置102-1からの送信信号は、RFC

3261に準拠したSIPメッセージの1つであるREGISTERメソッド400であって、そのメッセージに通信装置の位置情報が、要望する有効時間と共に設定されている(402)。また、公開鍵証明書要求と、ユーザ認証キーも設定されている(402)。これらの情報は、機密性を保つために、コンテンツ暗号化鍵で暗号化され、S/MIMEのEnveloped-Data(401)として送信される。

コンテンツ暗号化鍵の暗号化のための、鍵暗号化鍵としては、セッション制御サーバ101-1の公開鍵を用いてもよいし、セッション制御サーバ101-1と通信装置102-1の使用者間の事前共有鍵(パスワードなど)を用いてもよい。

【0017】

図5に示すように、セッション制御サーバ101-1からの受信信号は、REGISTERメソッドに対する正常応答200 OK(500)であって、そのメッセージに登録された位置情報と、セッション制御サーバ101-1が認めた有効時間が共に設定されている(504)。また、公開鍵証明書も設定されている(504)。これらの情報は、機密性を保つために、暗号化鍵で暗号化され、EnvelopedData内に設定されている(502)。

信号の復号化には、まず暗号化されたコンテンツ暗号化鍵(505)の復号化を行う。

暗号化鍵の復号化には、通信装置102-1の秘密鍵を用いてもよいし、セッション制御サーバ101-1と通信装置102-1の使用者間の事前共有鍵(パスワードなど)を用いてもよい。

復号化したコンテンツ暗号化鍵で、暗号化した情報(504)を復号化する。

受信した位置情報と公開鍵証明書は、有効時間とともに、位置情報と公開鍵証明書保管手段116に保管される。

改竄を防ぐために、サーバのデジタル署名(503)が添付されていれば、その署名を確認してもよい。

【0018】

(セッション制御サーバ)

図3は、本発明の実施形態に係るセッション制御サーバのブロック図である。

図3に示すように、セッション制御サーバ101は、信号受信手段120、セッション制御手段121、信号送信手段122、証明書発行（登録）要求受信手段123、証明書発行（有効性確認）手段124、位置登録要求受信手段125、位置情報と公開鍵証明書保管手段126、公開鍵証明書問合せ要求受信手段127、および、公開鍵証明書通知送信手段128を具備している。

ここで、123は、証明書発行要求受信手段と証明書登録要求手段の両方の機能を備えており、124は、証明書発行手段と証明書有効性確認手段の両方の機能を備えている。なお、123、124は、両方の機能のうち的一方だけを備えていてもよい。

【0019】

通信装置102-1からの位置登録要求信号を、信号受信手段120より受信する。受信した位置登録要求信号は、セッション制御手段121で位置登録要求信号であると分析されると、位置登録要求受信手段125に送られる。

位置登録要求手段125にて、ユーザ認証正常終了後、証明書発行要求が添付されていると判断されると、証明書発行要求受信手段123に必要な情報を提供する。証明書発行要求受信手段123は、要求内容が正当であることを確認し、証明書発行手段124にて、ユーザに対する証明書発行を行う。

発行した証明書と位置情報は、位置情報と公開証明書保管手段126にて保管される。

セッション制御手段121で、位置情報と公開鍵証明書の情報を含めた応答信号を生成し、通信装置102-1に信号送信する。

【0020】

（第2の実施形態）

第2の実施形態は、セッション制御サーバ101-1が、通信装置102-1から位置登録+証明書発行の要求を受け、通信装置102-1に位置登録と証明書発行の完了通知を送信するまでのやりとりである。

図4および図5は、前述のように、通信装置102-1からセッション制御サーバ101-1に送信する信号例と通信装置102-1がセッション制御サーバ

101-1 から受信する信号例であったので、セッション制御サーバ101-1 から通信装置102-1 に送信する信号例が図5、通信装置102-1 から受信する信号例が図4 になる。

【0021】

図4 に示すように、例えば、セッション制御サーバ101-1 が通信装置102-1 から受信した信号が、RFC3261 に準拠したSIPメッセージの1つであるREGISTERメソッドであって、そのメッセージに通信装置の位置情報が有効時間と共に設定されている(402)。また、公開鍵証明書要求と、ユーザ認証キーも設定されている(402)。これらの情報は、機密性を保つために、暗号化鍵で暗号化されている。

【0022】

コンテンツ暗号化鍵を取得するために、まず、暗号化されたコンテンツ暗号化鍵の復号化を行う。

セッション制御サーバ101-1 の秘密鍵を用いてもよいし、セッション制御サーバ101-1 と通信装置102-1 の使用者間の事前共有鍵(パスワードなど)を用いてもよい。

復号化して取得された暗号化鍵を用いて、暗号化された情報の復号化を行う。

復号化して取得された位置情報登録要求、ユーザ認証キー、証明書発行要求を得る。

ユーザ認証後、証明書発行要求が正当であることを確認し、セッション制御サーバ101-1 が発行元となる公開鍵証明書を発行する。

発行した公開鍵証明書の有効期限(504)は、位置情報の有効期限と同一に設定する。

そして、位置情報と公開鍵証明書を有効期限とともに保管する。

【0023】

図5 に示すように、REGISTERメソッドに対する正常応答200 OK(500)に、登録された位置情報と、セッション制御サーバ101-1 が認めた有効時間を共に設定する(504)。また、公開鍵証明書も設定する(504)。これらの情報は、機密性を保つために、暗号化鍵で暗号化する。信号の暗号

化には、暗号化鍵を生成し、その暗号化鍵の暗号化には、通信装置 102-1 の公開鍵を用いてもよいし、セッション制御サーバ 101-1 と通信装置 102-1 の使用者間の事前共有鍵（パスワードなど）を用いてもよい。

このように生成した信号を、通信装置 102-1 に送信する。

【0024】

図 8 は、第 2 の実施形態に係る通信装置の位置登録と証明書発行処理のフローチャートである。

通信装置から送信する信号について、暗号化・復号化などが行われるが、ここではその処理は記載を省略している。

まず、通信装置 102-1 は、通信装置 102-1 の位置登録要求を行うため、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求を一括して、位置登録+証明書発行要求信号をセッション制御サーバ 101-1 に送信する（51）（8-①）。セッション制御サーバ 101-1 は、この信号を受信し（52）、セッション制御を行い（53）、信号種別を判定して（54）、位置登録要求であれば、位置登録要求を受信し（55）、証明書発行要求があるか否かを判定し（56）、証明書発行要求がなければ、位置情報+証明書を管理する（59）。また、証明書発行要求があれば、証明書発行要求を受信し（57）、証明書を発行し（58）、位置情報+証明書を管理する（59）。そして、セッション制御を行い（60）、通信装置 102-1 に信号送信する（61）（8-②）。通信装置 102-1 は、位置登録+証明書発行完了通知を受信する（62）。

【0025】

（第 3 の実施形態）

第 3 の実施形態は、他のセッション制御サーバ 101-2 が通信装置 102-2 から受信した信号が、SIP に準拠した SIP メッセージの 1 つである OPTIONS メソッドであって、そのメッセージに通信装置 102-1 の公開鍵証明書問合せ要求が設定されている場合のやりとりである。

図 6 は、図 3 のセッション制御サーバの受信信号例を示す図であり、図 7 は、同じくセッション制御サーバの送信信号例を示す図である。

問合せ内容の改竄を防止するために、通信装置 102-2 のデジタル署名、ならびに署名検証のための通信装置 102-2 の公開鍵証明書が設定されている (604)。セッション制御サーバ 101-2 は、OPTIONS メソッドの Request-URI に設定されているドメイン名を見て、自ドメイン宛のメソッドか否かを判定する。自ドメインでない場合には、ドメイン名を示すセッション制御サーバ 101-1 に送信する。

【0026】

セッション制御サーバ 101-1 は、OPTIONS メソッドを受信して、OPTIONS メソッドの Request-URI に設定されているドメイン名を見て、自ドメイン宛のメソッドか否かを判定する。自ドメイン宛のメソッドであれば、証明書登録要求であるか否かを判別する。証明書登録要求であれば、位置情報と公開鍵証明書を保管手段 126 において、通信装置 102-1 のユーザの位置情報と公開鍵証明書と有効時間を検索し、その時点で有効な情報を取得する。それらを取得した情報を、図 7 に示す OPTIONS メソッドに対する応答 200 OK に設定して、通信装置 102-2 に送信する。

この場合、通信装置 102-2 に直接、送信することもできるが、ここではセッション制御サーバ 101-2 を経由して送信する。

【0027】

図 9 は、本発明の第 3 の実施形態に係る証明書問い合わせ処理のフローチャートである。

通信装置 102-2 は、証明書問合せ要求信号をセッション制御サーバ 101-2 に送信する (81) (9-①)。セッション制御サーバ 101-2 は、信号を受信すると (82)、セッション制御を行い (83)、自ドメイン宛か否かを判定し (84)、自ドメイン宛でなければ、セッション制御を行って (89)、該当するセッション制御サーバに送信する (90)。この場合、宛先であるセッション制御サーバ 101-1 に転送する (9-②)。自ドメイン宛であれば、信号種別を判定し (85)、証明書問合せ要求であれば、証明書問合せ要求を受信し (86)、証明書があるか否かを判定し (87)、証明書があれば、証明書の通知を行い (88)、セッション制御を行って (89)、通信装置 102-2 に

信号送信する(90)(9-④)。

【0028】

セッション制御サーバ101-1は、その信号を受信し(91)、セッション制御を行い(92)、自ドメイン宛であるか否かを判定し(93)、自ドメイン宛でなければ、セッション制御を行って(98)、セッション制御サーバ101-2に送信するか(99)、廃棄する。自ドメイン宛であれば、信号種別を判定し(94)、証明書問合せ要求であれば、証明書問合せ要求を受信する(95)。証明書があるか否かを判定し(96)、あれば、証明書通知を行い(97)、セッション制御を行って(98)、セッション制御サーバ101-2に信号送信する(99)(9-③)。

セッション制御サーバ101-2は、これを受信すると(82)、セッション制御を行い(83)、自ドメイン宛でないので、宛先である通信装置102に対して信号送信する(90)(9-④)。通信装置102-2は、この証明書通知を受信する(100)。

【0029】

このように、本実施形態に係る通信方法では、通信装置で有効な公開鍵証明書をセッション制御サーバで管理することで、セッション通信で利用可能な電子証明書(公開鍵証明書)の配布・流通が可能となる。

また、セッション制御サーバによる電子証明書の配布時に、セッション制御サーバにより有効性が確認されているため、セッション制御信号内で使用する電子証明書の有効性を、認証局などに問い合わせることなく、確認することが可能となる。

なお、図8および図9の動作フローをプログラム化した後、これらのプログラムをCD-ROMなどの記録媒体に格納しておけば、プログラムの販売や貸与の場合に便利であり、また、セッション制御サーバとなるコンピュータや、通信装置のコンピュータにこの記録媒体を装着して、プログラムをインストールし、プログラムを実行させることにより、本発明を容易に実現することができる。

【0030】

【発明の効果】

以上説明したように、本発明によれば、通信装置間の機密性の高い信号送受信のために必要な電子証明書（公開鍵証明書）を、セッション制御サーバが通信装置対応の有効性を確認した上で、これを管理するので、実利用可能な電子証明書の配布が可能であり、ユーザへのセッション確立時の有効性確認が容易となる。

【図面の簡単な説明】

【図 1】

本発明の実施形態に係る通信システムの構成図である。

【図 2】

図 1 における通信装置の詳細ブロック構成図である。

【図 3】

図 1 におけるセッション制御サーバの詳細ブロック構成図である。

【図 4】

本発明の第 1 の実施形態に係る通信装置の送信信号例を示す図である。

【図 5】

本発明の第 1 の実施形態に係る通信装置の受信信号例を示す図である。

【図 6】

本発明の第 3 の実施形態に係るセッション制御サーバの受信信号例を示す図である。

【図 7】

本発明の第 3 の実施形態に係るセッション制御サーバの送信信号例を示す図である。

【図 8】

本発明の第 2 の実施形態に係るセッション制御サーバと通信装置の処理フローチャートである。

【図 9】

本発明の第 3 の実施形態に係るセッション制御サーバと通信装置の処理フローチャートである。

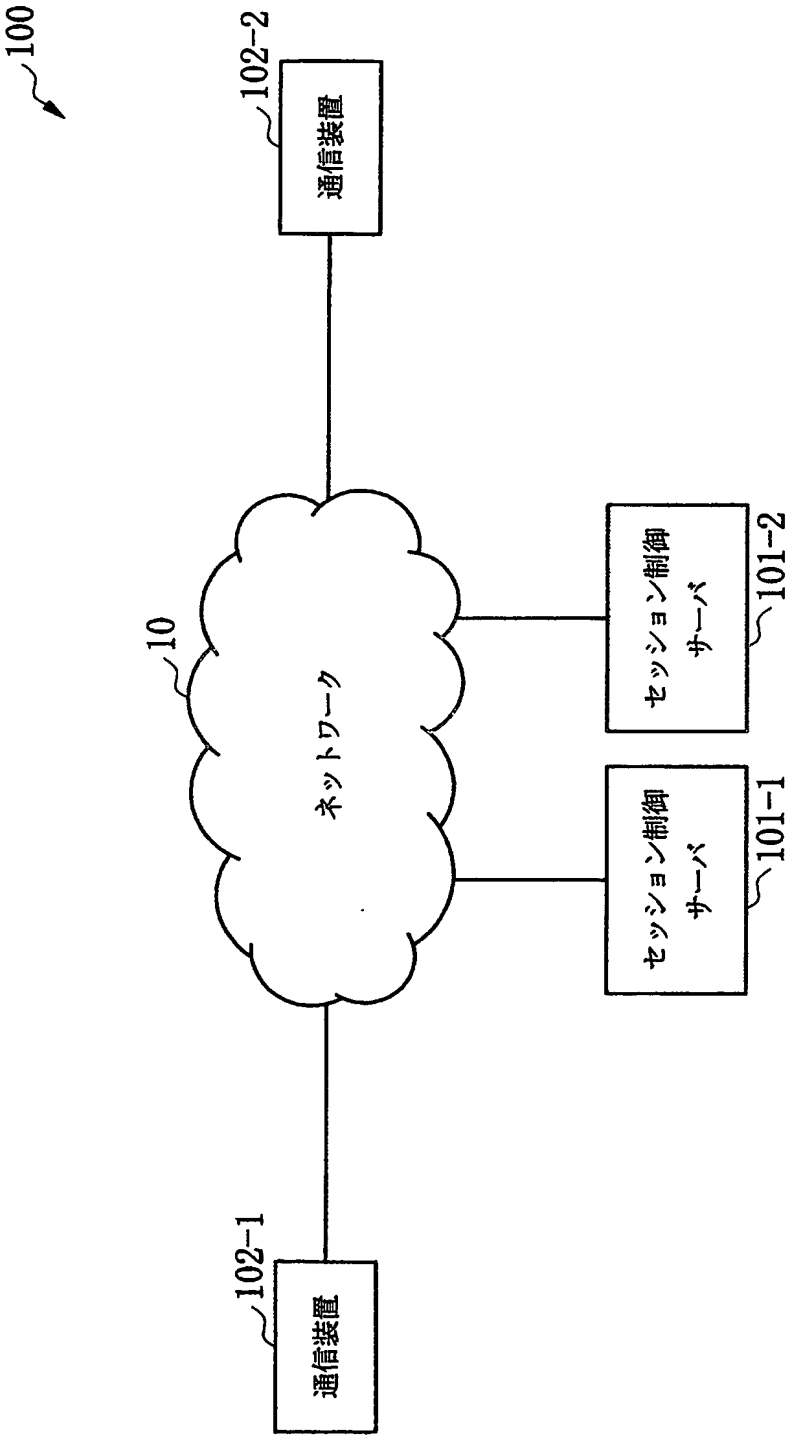
【符号の説明】

10…ネットワーク、101…セッション制御サーバ、102…通信装置、

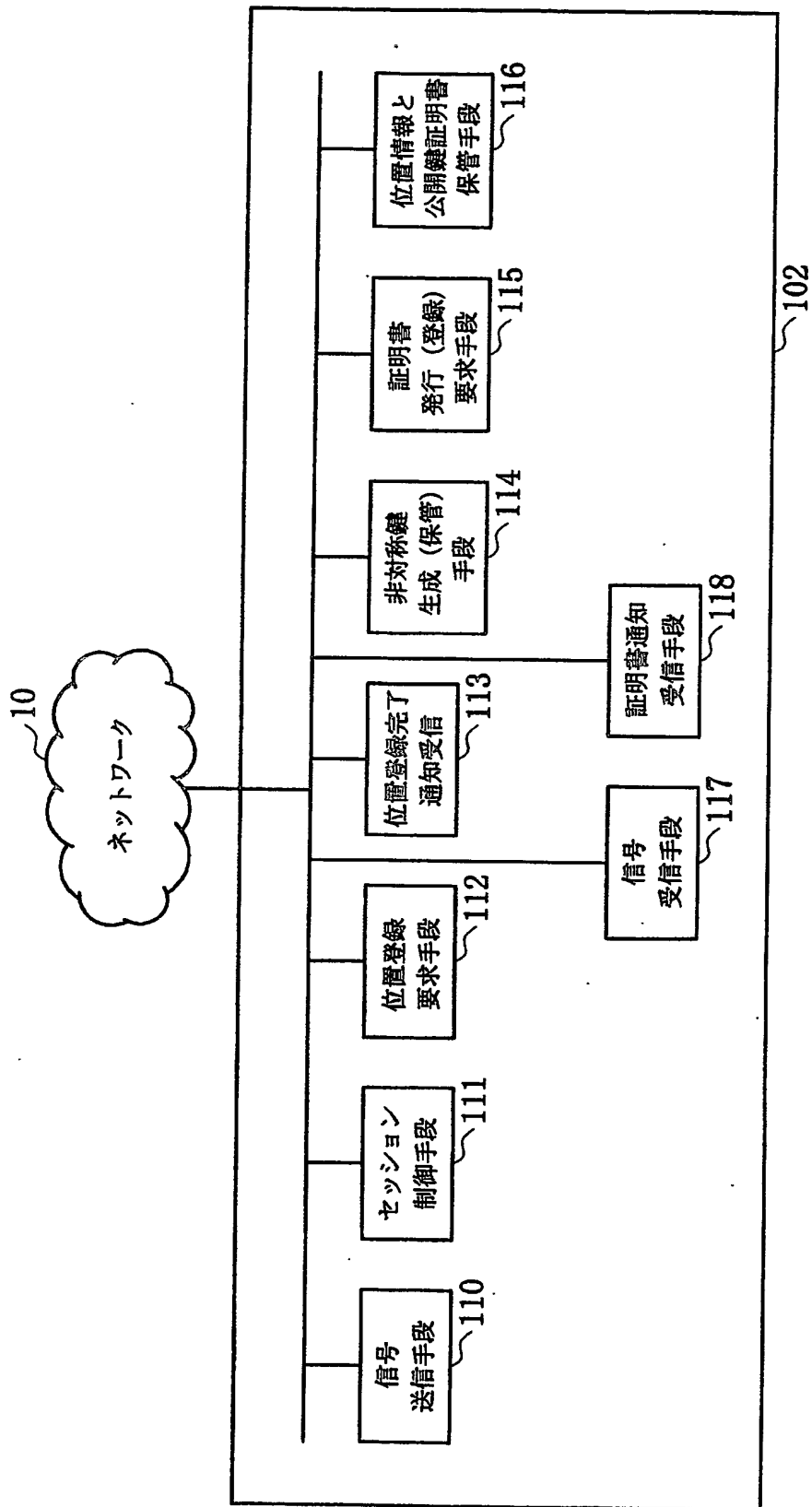
1 0 1 - 1 …通信装置 1 0 2 - 1 を収容するセッション制御サーバ、
1 0 1 - 2 …通信装置 1 0 2 - 2 を収容するセッション制御サーバ、
1 0 2 - 1 …発信側通信装置、1 0 2 - 2 …着信側通信装置、
1 1 0 …信号送信手段、1 1 1 …セッション制御手段、
1 1 2 …位置登録要求手段、1 1 3 …位置登録完了通知受信手段、
1 1 4 …非対称鍵生成（保管）手段、1 1 5 …証明書発行（登録）手段、
1 1 6 …位置情報と公開鍵証明書保管手段、1 1 7 …信号受信手段、
1 1 8 …証明書通知受信手段、1 2 0 …信号受信手段、
1 2 1 …セッション制御手段、1 2 2 …信号送信手段、
1 2 3 …証明書登録要求受信手段、1 2 4 …証明書有効性確認手段、
1 2 5 …位置登録要求受信手段、1 2 6 …位置情報と公開鍵証明書保管手段、
1 2 7 …証明書問合せ要求受信手段、1 2 8 …証明書通知手段、
4 0 0 ～ 4 0 3 …証明書発行要求の信号例の各領域、
5 0 0 ～ 5 0 5 …証明書発行の信号例の各領域、
6 0 0 ～ 6 0 4 …証明書問合せ要求の信号例の各領域、
7 0 0 ～ 7 0 5 …証明書通知の信号例の各領域。

【書類名】 図面

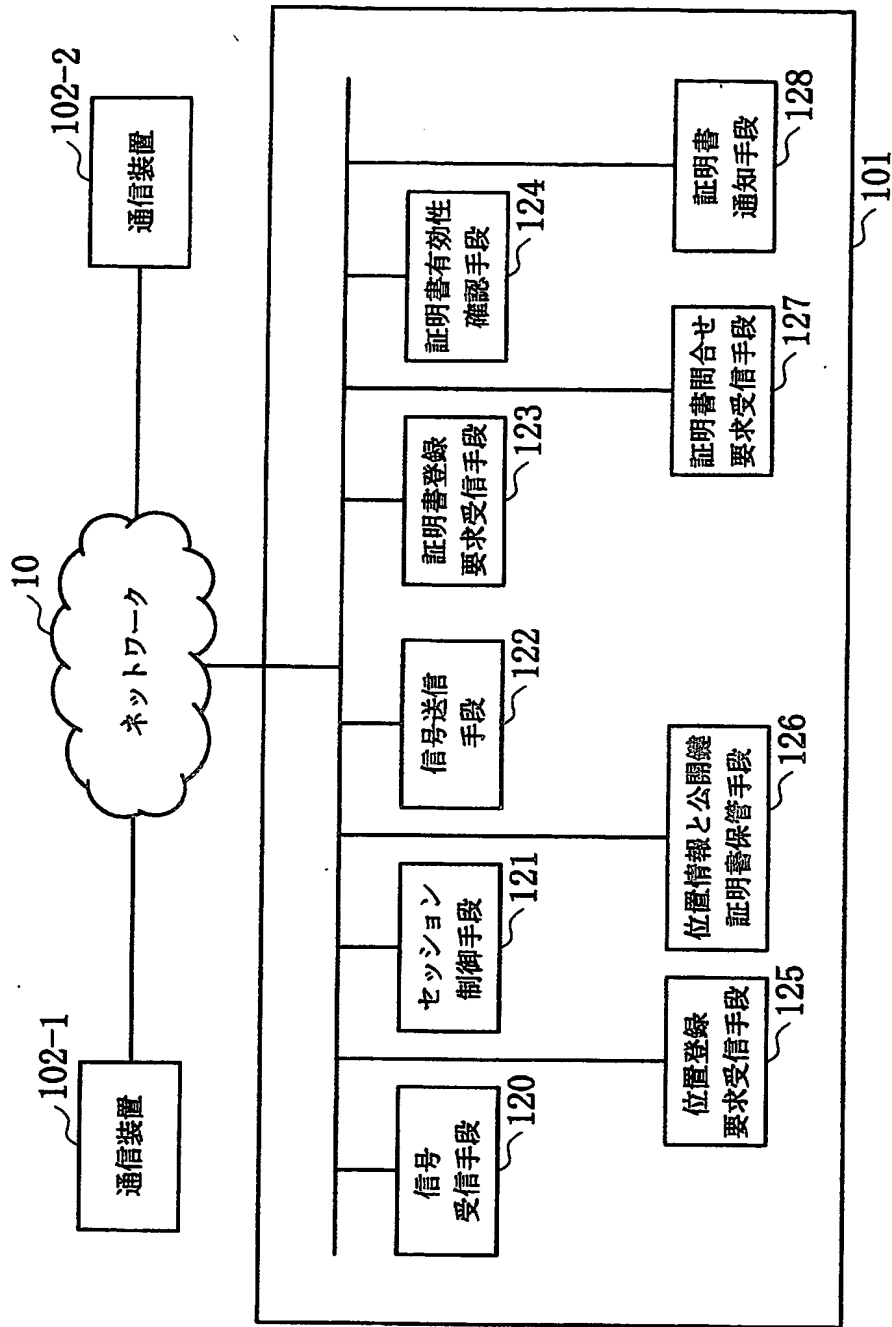
【図1】



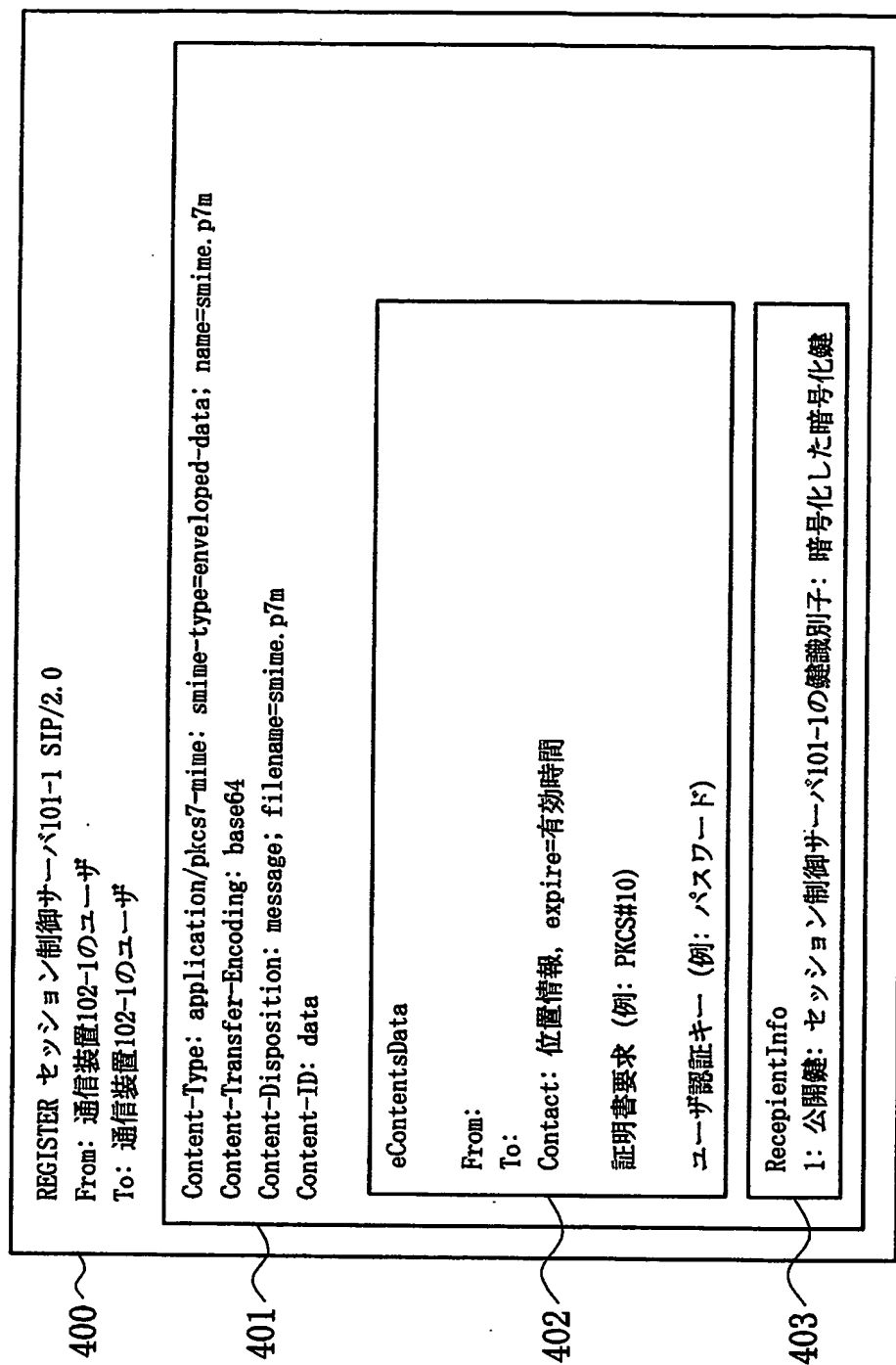
【図 2】



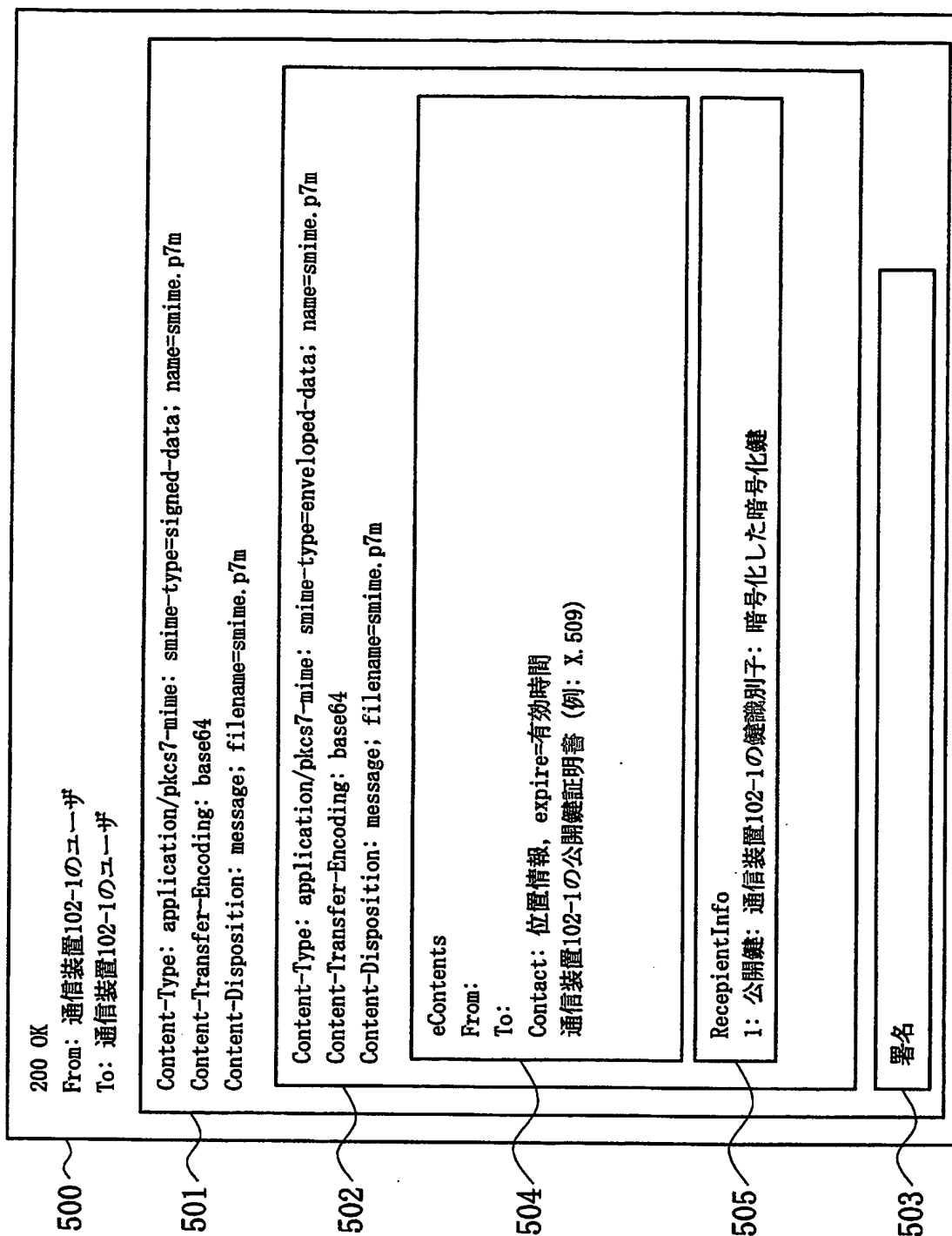
【図3】



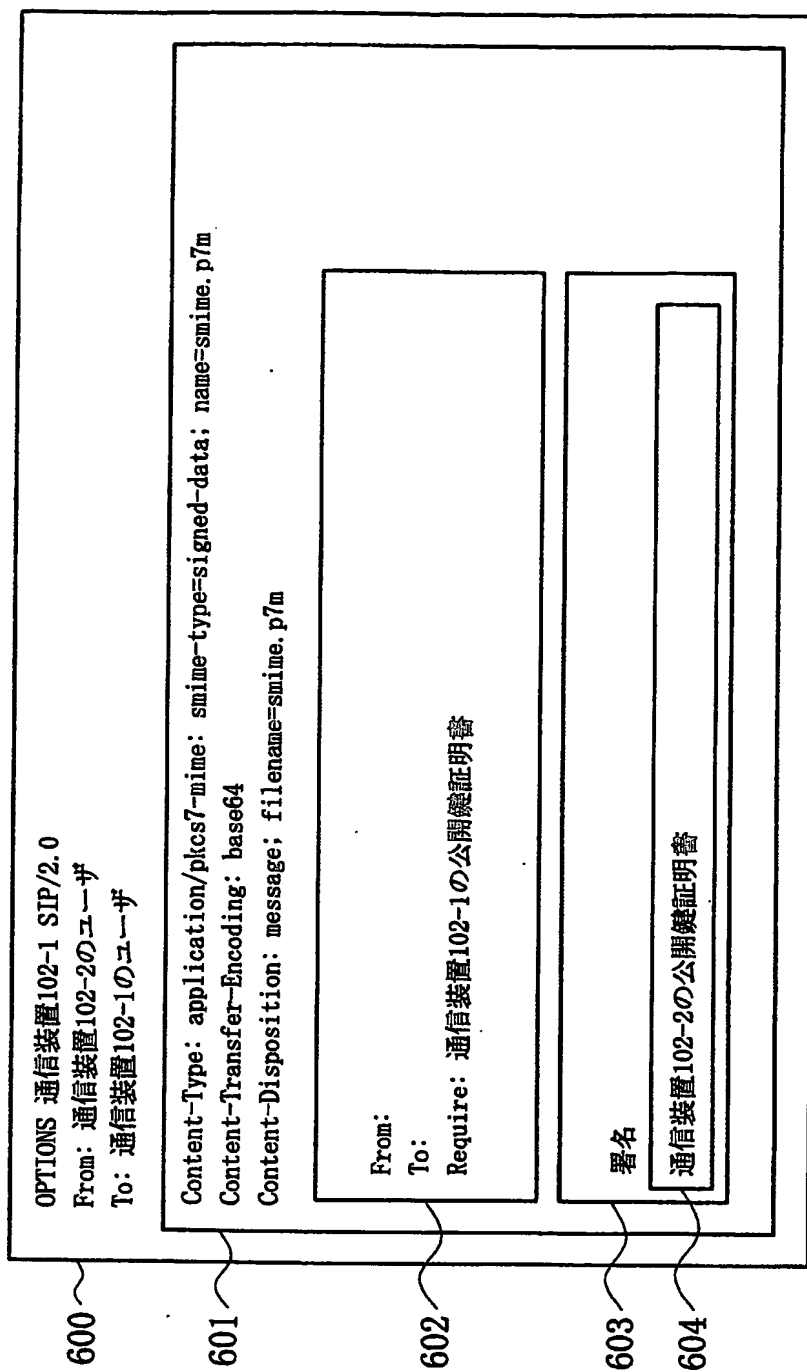
【図4】



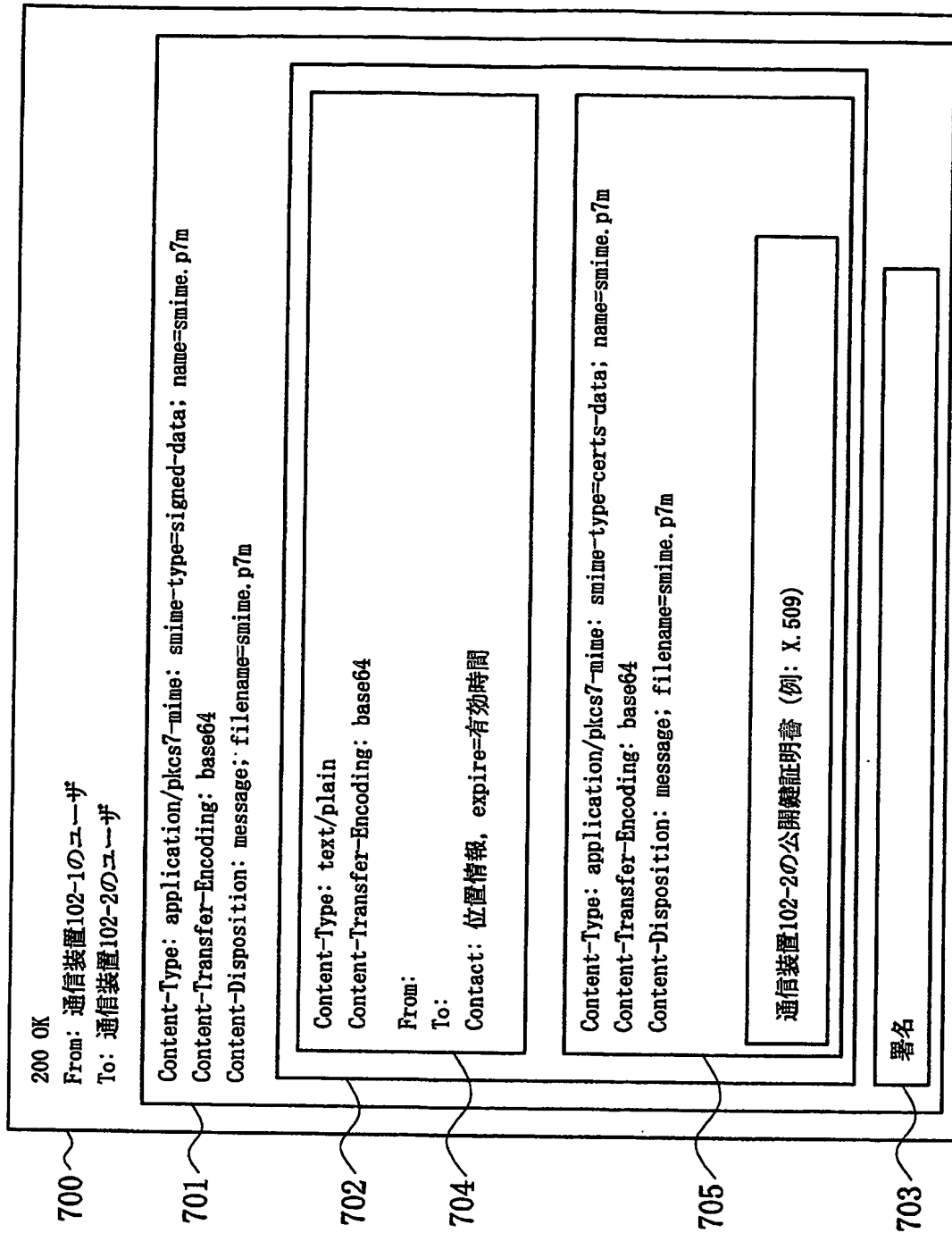
【図 5】



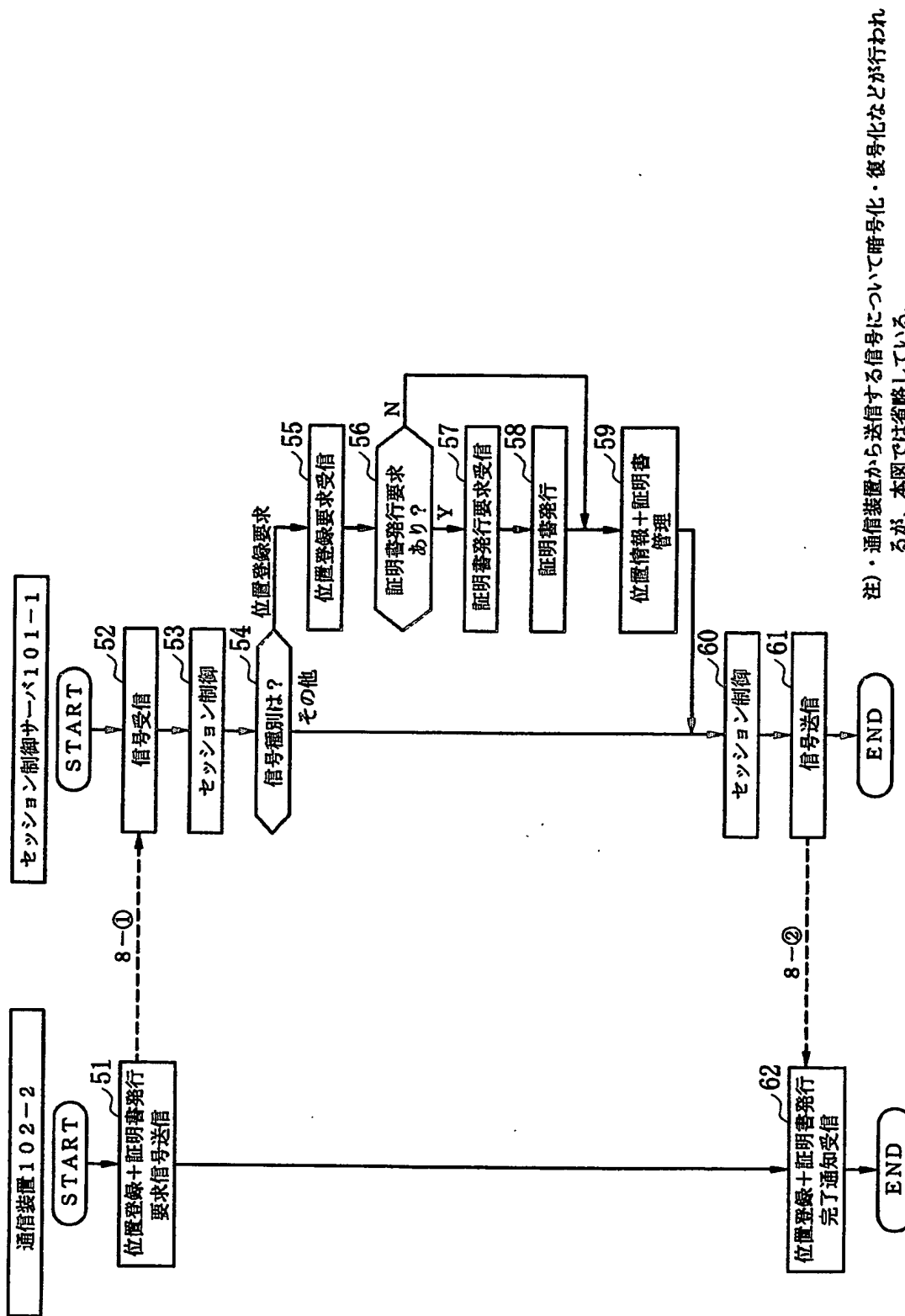
【図 6】



【図 7】

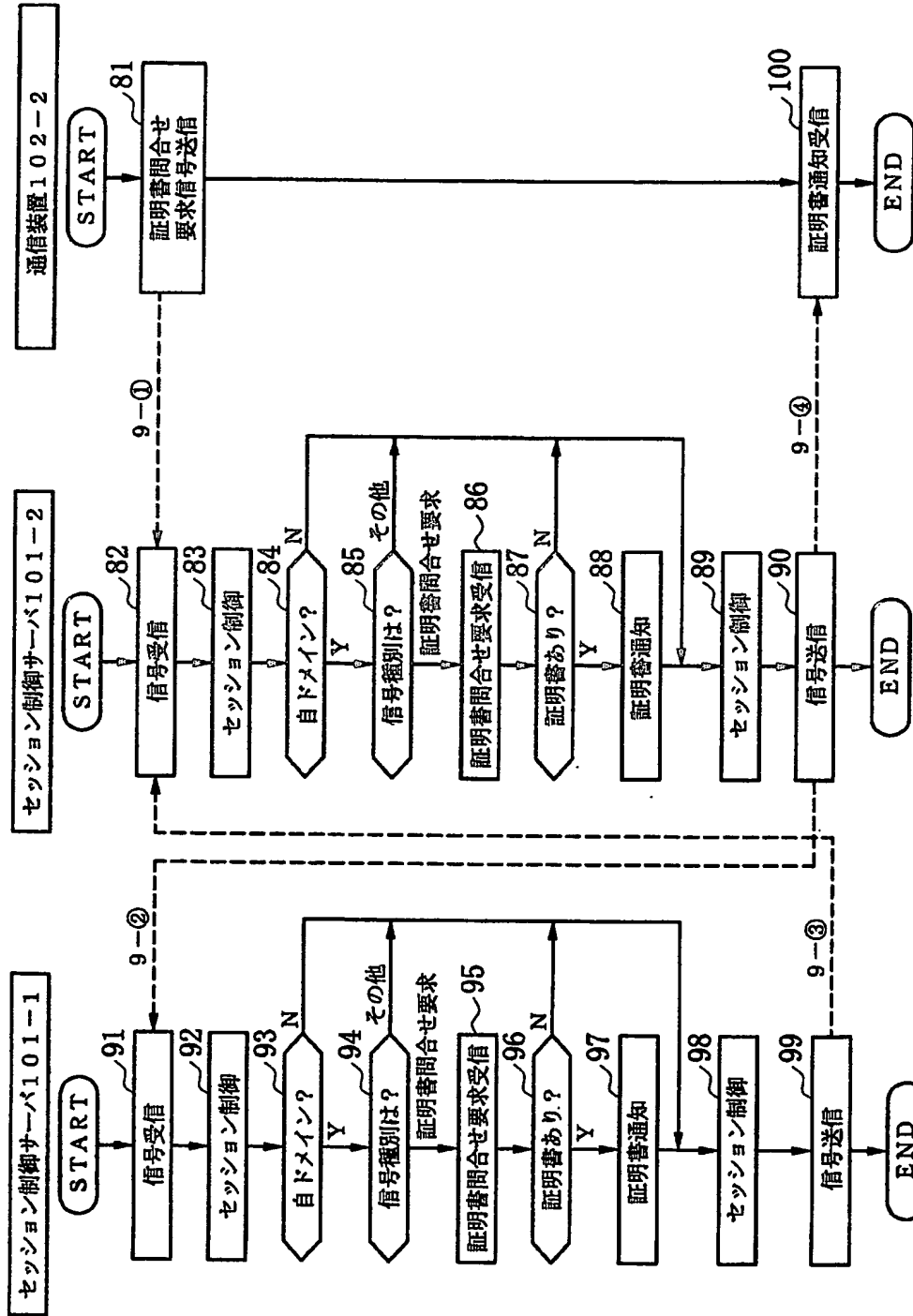


【図8】



注)・通信装置から送信する信号について暗号化・復号化などが行われるが、本図では省略している。

【図9】



注)・通信装置から送信する信号について暗号化・復号化などが行われるが、本図では省略している。

【書類名】 要約書

【要約】

【課題】 実利用可能な電子証明書の配布が可能であり、ユーザへのセッション確立時の有効性確認を容易にする。

【解決手段】 あるユーザが通信装置 102-1 の位置登録要求を行うため、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求を一括してセッション制御サーバ 101-1 に送信する。セッション制御サーバ 101-1 が要求を受信し、ユーザ認証した上で証明書を発行し、位置情報の有効時間とともに保管する。通信装置 102-1 はセッション制御サーバ 101-1 からの位置登録完了通知と、証明書発行完了通知を、有効時間とともに受信し、これを保管する。通信装置 102-2 がセッション開始に先立ち、通信相手 102-1 の公開証明書をセッション制御サーバ 101-2 に対して問い合わせると、これをセッション制御サーバ 101-1 に転送し、セッション制御サーバ 101-1 は、通信相手 102-1 について、公開鍵証明書の有効性を確認し、これを通信装置 102-2 に通知する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2003-175085
受付番号	50301026572
書類名	特許願
担当官	第八担当上席 0097
作成日	平成15年 6月20日

<認定情報・付加情報>

【提出日】	平成15年 6月19日
-------	-------------

次頁無

出 願 人 履 歴 情 報

識別番号

[000004226]

1. 変更年月日

1999年 7月15日

[変更理由]

住所変更

住 所

東京都千代田区大手町二丁目3番1号

氏 名

日本電信電話株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.